日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月２７日

出願番号
Application Number: 特願２０００－３９８８５９

出願人
Applicant(s): 株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ４月２０日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

【書類名】　特許願
【整理番号】　A000006672
【提出日】　平成12年12月27日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L　9/00
【発明の名称】　通信装置、及びその認証方法
【請求項の数】　20
【発明者】
【住所又は居所】　東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
【氏名】　青柳　和則
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【弁理士】
【氏名又は名称】　坪井　淳
【選任した代理人】
【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信装置、及びその認証方法

【特許請求の範囲】

【請求項１】　認証コード記憶手段と、

前記認証コード記憶手段に記憶されている認証コードを用いて認証を行なう手段と、

認証が成功した場合、新たな認証コードを演算し、前記認証コード記憶手段に記憶されている認証コードを更新する認証コード更新手段と、

を具備することを特徴とする通信装置。

【請求項２】　入力された認証コードを第１の認証コードと照合し、両者が不一致の場合、認証を終了する手段と、

両者が一致した場合、前記認証手段と認証コード更新手段とを動作させる手段とを具備することを特徴とする請求項１記載の通信装置。

【請求項３】　前記認証コード記憶手段に認証コードが記憶されていない場合、前記認証手段は前記入力された認証コードを用いて通信装置の認証を行なうことを特徴とする請求項２記載の通信装置。

【請求項４】　前記認証手段は、認証される装置固有の情報と、認証コードとを用いて認証を行ない、前記認証コード記憶手段に通信装置毎の認証データが記憶されていない場合は、認証に使われる認証コードとしては前記入力された認証コードを使うことを特徴とする請求項２記載の通信装置。

【請求項５】　前記認証手段は、前記認証コードと認証される装置固有の情報とに基づいて認証データを演算し、認証される装置の認証データとの照合を行なうことを特徴とする請求項１記載の通信装置。

【請求項６】　前記認証手段は、前記認証コードと前記固有情報と乱数とに基づいて認証データを演算することを特徴とする請求項５記載の通信装置。

【請求項７】　前記認証コード更新手段は、前記認証コード記憶手段に記憶され認証に使われた認証コードに所定の演算を施し、新たな認証コードを生成することを特徴とする請求項１記載の通信装置。

【請求項８】　前記認証コード更新手段は、前記認証コード記憶手段に記憶

され認証に使われた認証コードと乱数とに所定の演算を施し、新たな認証コードを生成することを特徴とする請求項７記載の通信装置。

【請求項９】　２台の通信装置間の認証方法において、

認証を求める装置から認証を受ける装置へ所定のデータを送信し、２台の通信装置の各々において、前記所定のデータと演算用の認証コードと認証を受ける装置固有の情報とに第１の演算を施し、認証データを演算し、両装置の認証データを照合し、

両装置の認証データが一致した場合、前記２台の通信装置の各々において、前記所定のデータと演算用の認証コードに第２の演算を施し、演算用の認証コードを更新することを特徴とする通信装置の認証方法。

【請求項１０】　各々の通信装置において入力された認証コードを所定の認証コードと照合し、不一致の場合は認証を終了させることを特徴とする請求項９に記載の通信装置の認証方法。

【請求項１１】　前記演算用の認証コードの初期値は入力された認証コードであることを特徴とする請求項９に記載の通信装置の認証方法。

【請求項１２】　前記所定のデータは乱数であることを特徴とする請求項９に記載の通信装置の認証方法。

【請求項１３】　他の通信装置を認証する機能を有する通信装置において、

入力された第１のコード、あるいは予め記憶された第１のコードを所定のコードと照合し、両者が不一致の場合、認証を終了する手段と、

両者が一致した場合、該他の通信装置へ乱数を送信する手段と、

前記乱数と認証用のコードと該他の通信装置の識別データとに基づいて認証データを演算し、該他の通信装置から送信された認証データと照合する手段と、

両通信装置の認証データが一致した場合、前記乱数と認証用のコードとに基づいて認証コードを更新する手段と、

を具備することを特徴とする通信装置。

【請求項１４】　前記更新された認証コードは記憶手段に記憶され、前記照合手段は記憶手段に認証用のコードが記憶されていない場合は第１のコードを用いることを特徴とする請求項１３に記載の通信装置。

【請求項１５】　他の通信装置から認証が要求されると、入力された第１のコード、あるいは予め記憶された第１のコードを所定のコードと照合し、両者が不一致の場合、終了する手段と、

該他の通信装置から乱数を受信する手段と、

前記乱数と認証用のコードと自装置の識別データとに基づいて認証データを演算し、該他の通信装置へ認証データを送信する手段と、

該他の通信装置から認証の結果を受信し、認証成功の場合、前記乱数と認証用のコードとに基づいて認証コードを更新する手段と、

を具備することを特徴とする通信装置。

【請求項１６】　前記更新された認証コードは記憶手段に記憶され、前記送信手段は記憶手段に認証用のコードが記憶されていない場合は第１のコードを用いることを特徴とする請求項１５に記載の通信装置。

【請求項１７】　認証用のコードを用いて２台の通信装置間で互いに認証を行なわせるプログラムコード手段と、

認証が成功した場合、新たな認証コードを演算し、認証用のコードを更新させるプログラムコード手段と、

を具備することを特徴とする通信装置の認証プログラムを記憶した記録媒体。

【請求項１８】　前記認証プログラムコード手段は、２台の通信装置で共有している認証用のコードと、一方の通信装置に固有の情報と、一方の通信装置で発生され他の通信装置に送信される所定のコードとに基づいて認証データを演算し、２台の通信装置の認証データを照合することを特徴とする請求項１７に記載の記録媒体。

【請求項１９】　第１認証コードを入力する入力手段と、

この入力手段にて入力された上記第１認証コードに対応した第２認証コードを出力する出力手段と、

この出力手段にて出力された上記第２認証コードを用いて外部機器との間で通信リンク設定のための認証を行なう認証手段と、

この認証手段による認証が成功した場合、上記第２認証コードを、上記出力手段が出力したものと異なるものに更新する更新手段と、

を具備することを特徴とする通信装置。

【請求項２０】　第１認証コードを入力するステップと、

この入力ステップにて入力された上記第１認証コードに対応した第２認証コードを出力するステップと、

この出力ステップにて出力された上記第２認証コードを用いて外部機器との間で通信リンク設定のための認証を行なうステップと、

この認証ステップによる認証が成功した場合、前記認証ステップで用いられる上記第２認証コードを、上記出力ステップが出力したものと異なるものに更新する更新ステップと、

を具備することを特徴とする通信装置の認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は通信装置に関し、特に通信相手の無線通信装置との通信が許可されているかどうかを判定する認証方法に関する。

【０００２】

【従来の技術】

無線通信は不特定多数の相手と通信が可能であるので、複数の無線通信装置間で通信を行なう際、通信を許可していない第三者に通信内容を取得（傍受）されるのを防ぎたい場合がある。この場合、無線通信装置間で認証データ（パスワードや装置固有の識別番号等に基づいたデータ）を予め交換し、認証された無線通信装置間でしか通信できないようにしたり、暗号化用の鍵データを予め交換し、その鍵データに基づいて通信データを暗号化して通信する等の方法がとられている。

【０００３】

近距離無線通信方式の一つであるＢｌｕｅｔｏｏｔｈ（ver.1）では、日刊工業新聞社発行の「ワイヤレス通信の新技術Ｂｌｕｅｔｏｏｔｈガイドブック」（宮津和弘著）に記載のように、認証データを予め交換し、認証された無線通信装置間でしか通信できないようにしている。

【０００４】

具体的には、発信元の無線通信装置Ａから通話相手である無線通信装置Ｂへ接続要求を送信し、無線通信装置Ｂが接続要求を受信する。なお、通信を許可し合う無線通信装置Ａ、Ｂは共通の認証コードを共有しているとする。

【０００５】

無線通信装置Ａ、Ｂそれぞれにおいて認証コードを入力する。認証コードはキーボード等のユーザーインターフェースを使って入力する場合や、通信装置内部のメモリに予め記憶されているものを利用する場合がある。

【０００６】

無線通信装置Ａにおいて認証用乱数を発生し、無線通信装置Ｂへ送信し、無線通信装置Ｂがこの認証用乱数を受信する。各無線通信装置は無線通信装置Ｂの識別番号、認証コード、認証用乱数をパラメータとして認証データを演算する。

【０００７】

無線通信装置Ｂは認証データを発信元の無線通信装置Ａへ送信し、無線通信装置Ａはその認証データを受信する。

【０００８】

無線通信装置Ａは先に受信した無線通信装置Ｂが演算した認証データと、自身が演算した認証データとを照合する。ここで、通信を許可した無線通信装置Ｂ以外の無線通信装置は認証コードを知らないので、正しい認証データを演算することができない。そのため、これらの認証データが一致したら、認証が成功したとみなし、認証が成功したことを無線通信装置Ｂに通知する。認証データが一致しなかった場合は、認証に失敗したとみなし、認証の失敗を無線通信装置Ｂに通知する。無線通信装置Ｂは無線通信装置Ａからの認証結果の通知（成功、失敗）を受信し、認証が成功したか失敗したかを判断する。認証が成功した場合、無線通信装置Ａ、Ｂ間でデータの送受信を行なう。認証に失敗した場合は、接続が完了せず、データ送受信は行なわない。　ここで、認証に使うパラメータのうち、認証コードはユーザーインターフェースにより直接入力するので、第三者に傍受されることはない。しかし、通信相手の無線通信装置Ｂの識別番号は認証開始前にあらかじめ取得できるものであり、例えばＢｌｕｅｔｏｏｔｈではＩｎｑｕｉｒ

ｙという動作により、周辺にあるＢｌｕｅｔｏｏｔｈに準拠した無線通信装置の識別番号を取得することができるので、第三者に傍受される可能性がある。また、認証用乱数や演算結果である認証データも無線で交換するので、第三者に傍受される可能性がある。

【０００９】

そのため、乱数、無線通信装置の識別番号、それらをパラメータとする演算結果である認証データを傍受された場合、演算結果から認証コードを逆算されるおそれがある。認証コードや無線通信装置の識別番号を入手した第三者は、新たな無線通信装置を用意して当該識別番号の無線通信装置に成り済まして不正な無線通信を行なうことも可能になる。

【００１０】

このような不正通信を防ぐことを目的とする無線電話装置が特開平７－１６２９５０号で提案されている。ここでは、通信網に接続された第１の無線装置（親機）と少なくとも１つの第２の無線装置（子機）との間で無線信号を用いて通信を行なう無線電話装置において、第２の無線装置が、第１の無線装置が生成し出力した認証コードと、第２の無線装置に記憶された暗証コードとに基づいて、予め決められた方法で符号化した認証符号を出力するように構成し、第１の無線装置が、第１の無線装置に記憶された暗証コードおよび認証コードに基づいて第２の無線装置が出力した認証符号の符号化の正否を判定し、正しい符号化による認証符号であると判定した場合に、第２の無線装置に通話を許可する構成としている。

【００１１】

しかし、この従来例においても、認証コードが傍受されると、予め記憶している暗証コードとから認証符号が逆演算により解析できてしまい、以降の不正接続を防止できない。

【００１２】

【発明が解決しようとする課題】

このように従来の無線通信装置の認証では、傍受により認証データを演算するパラメータの取得が可能であり、成り済ましによる不正な通信が行われるおそれ

がある。なお、この問題は無線通信装置に限らず、有線の通信装置についても生じるおそれがある。

【００１３】

本発明は上述した事情に対処すべくなされたもので、その目的は第三者が通信を傍受して認証のためのデータを解析しても成り済ましによる不正な通信を防ぐことができる通信装置、及びその認証方法を提供することである。

【００１４】

【課題を解決するための手段】

上記した課題を解決し目的を達成するために、本発明は以下に示す手段を用いている。

【００１５】

（１）認証コード記憶手段と、前記認証コード記憶手段に記憶されている認証コードを用いて認証を行なう手段と、認証が成功した場合、新たな認証コードを演算し、前記認証コード記憶手段に記憶されている認証コードを更新する認証コード更新手段とを具備する通信装置。

【００１６】

（２）２台の通信装置間の認証方法において、認証を求める装置から認証を受ける装置へ所定のデータを送信し、２台の通信装置の各々において、前記所定のデータと演算用の認証コードと認証を受ける装置固有の情報とに第１の演算を施し、認証データを演算し、両装置の認証データを照合し、両装置の認証データが一致した場合、前記２台の通信装置の各々において、前記所定のデータと演算用の認証コードに第２の演算を施し、演算用の認証コードを更新する。

【００１７】

（３）他の通信装置を認証する機能を有する通信装置において、入力された第１のコード、あるいは予め記憶された第１のコードを所定のコードと照合し、両者が不一致の場合、認証を終了する手段と、両者が一致した場合、該他の通信装置へ乱数を送信する手段と、前記乱数と認証用のコードと該他の通信装置の識別データとに基づいて認証データを演算し、該他の通信装置から送信された認証データと照合する手段と、両通信装置の認証データが一致した場合、前記乱数と認

証用のコードとに基づいて認証コードを更新する手段とを具備する。

【００１８】

（４）他の通信装置から認証が要求されると、入力された第１のコード、あるいは予め記憶された第１のコードを所定のコードと照合し、両者が不一致の場合、終了する手段と、該他の通信装置から乱数を受信する手段と、前記乱数と認証用のコードと自装置の識別データとに基づいて認証データを演算し、該他の通信装置へ認証データを送信する手段と、該他の通信装置から認証の結果を受信し、認証成功の場合、前記乱数と認証用のコードとに基づいて認証コードを更新する手段とを具備する通信装置。

【００１９】

（５）認証用のコードを用いて２台の通信装置間で互いに認証を行なわせるプログラムコード手段と、認証が成功した場合、新たな認証コードを演算し、認証用のコードを更新させるプログラムコード手段とを具備する通信装置の認証プログラムを記憶した記録媒体。

【００２０】

（６）第１認証コードを入力する入力手段と、この入力手段にて入力された上記第１認証コードに対応した第２認証コードを出力する出力手段と、この出力手段にて出力された上記第２認証コードを用いて外部機器との間で通信リンク設定のための認証を行なう認証手段と、この認証手段による認証が成功した場合、上記第２認証コードを、上記出力手段が出力したものと異なるものに更新する更新手段とを具備する通信装置。

【００２１】

（７）第１認証コードを入力するステップと、この入力ステップにて入力された上記第１認証コードに対応した第２認証コードを出力するステップと、この出力ステップにて出力された上記第２認証コードを用いて外部機器との間で通信リンク設定のための認証を行なうステップと、この認証ステップによる認証が成功した場合、前記認証ステップで用いられる上記第２認証コードを、上記出力ステップが出力したものと異なるものに更新する更新ステップとを具備する通信装置の認証方法。

【００２２】

本発明によれば、所定のパラメータから演算され認証に使うデータを認証の度、変更することにより、第三者が通信を傍受して認証に使ったデータを解析したとしても、次回の認証の際には認証データが更新されているので、解析した認証データが無効となって、不正な通信を防ぐことができる。

【００２３】

【発明の実施の形態】

以下、図面を参照して本発明による通信装置とその認証方法の実施形態を説明する。

【００２４】

第１実施形態

図１は本発明の第１実施形態に係る無線通信装置の一実施形態の構成を示すブロック図である。

【００２５】

ＣＰＵを含むデータ処理部４に無線部２、送信データ発生部３が接続される。無線部２にはアンテナ１が接続され、受信データの復調、送信データの変調等を行なう。送信データ発生部３は実際の通信データを生成し、データ処理部４、無線部２、アンテナ１を介して通信相手の無線通信装置にデータを送信する。キーボード等のユーザーインターフェースを持つ認証コード入力部８は認証コードを入力するために使われる。認証コード入力部８から入力された認証コードは認証コード記憶部７に格納される。なお、本実施形態では、認証コードは第１、第２の認証コードの２種類があり、認証コード入力部８から入力された認証コードは第１の認証コードとして認証コード記憶部７に格納される。第１の認証コードは認証には使われずに、第２の認証コードが認証に使われる。第２の認証コードは接続対象の無線通信装置毎に決まれており、初期値は第１の認証コードであるが、その後は認証の都度、更新される。この更新演算のために、認証コード演算部６が認証コード記憶部７に接続され、乱数発生部５から発生された乱数に基づいて第２の認証コードが更新される。認証コード記憶部７は第２の認証コードも記憶される。

【００２６】

図２に認証コード記憶部７の記憶内容を示す。第１の認証コードは、通信する装置グループ毎に異なるコードを設定したため、複数のコードを記憶している場合を示しているが、どのグループに対しても共通の第１の認証コードを用いる場合は単数でもよい。

【００２７】

データ処理部は、認証コード入力部８から入力された第１の認証コードが認証コード記憶部７に記憶されている第１認証コードと一致する場合、乱数発生部５で認証用乱数を発生させ、送受信データの処理を行なう。すなわち、データ処理部４は認証用乱数を無線部２に送る。無線部２は送信データの変調、受信データの復調等を行なう。次に、アンテナ１を介して通信対象となる無線通信装置へ認証用乱数を送信する。

【００２８】

一方、認証用乱数をアンテナ１を介して受信した通信相手の無線通信装置は、無線部２で受信データを復調し、復調データをデータ処理部４へ送る。データ処理部４では、受信した認証用乱数と、認証コード記憶部７に記憶されている第２認証コードと、自身の無線通信装置の識別番号とをパラメータとし、認証データを演算する。そして、その認証データを無線部２に送り、アンテナ１を介して発信元の無線通信装置へ認証データを送信する。

【００２９】

また、送信元の無線通信装置においても、データ処理部４において、自身が発生した認証用乱数と、第２認証コードと、通信相手の無線通信装置の識別番号とをパラメータとし、認証データを演算する。自身で演算した認証データと、アンテナ１、無線部２を介して受信した通信相手からの認証データとを照合する。両者が一致するなら、認証に成功したとみなし、データ処理部４から無線部２、アンテナ１を介して通信相手の無線通信装置へ認証成功の通知を送信する。その後、送信データ発生部３で実際に通信するデータを生成し、データ処理部４、無線部２、アンテナ１を介して通信相手の無線通信装置とデータ送受信を行なう。

【００３０】

また、認証に成功した場合は、認証開始時に乱数発生部５で発生させた乱数と、認証コード記憶部７に記憶されている第２認証コードとをパラメータとし、認証コード演算部６において新しい第２認証コードを演算し、認証コード記憶部７の第２認証コードを更新する。次回の認証時には、認証コード入力部８からは今までと同じ第１認証コードを入力するが、認証データの演算には第１認証データではなく更新された第２認証コードを使う。

【００３１】

次に、図３のフローチャートを参照して認証手順の詳細を説明する。ここでは、無線通信装置Ａが無線通信装置Ｂとの通信に先立って、認証を行なう場合を説明する。

【００３２】

無線通信装置Ａはステップ Ｓ１において無線通信装置Ｂの識別番号を指定して接続要求を送信する。無線通信装置Ｂはステップ Ｓ１５において、無線通信装置Ａからの接続要求を受信する。

【００３３】

ステップＳ２、Ｓ１６において、無線通信装置Ａ、Ｂそれぞれにおいて、図２に示されるような第１認証コードをそれぞれ入力する。ここでも、認証コードはキーボード等のユーザーインターフェースを使って入力する場合に限らず、通信装置内部のメモリに予め記憶されているものを利用してもよい。

【００３４】

ステップＳ３、Ｓ１７において、無線通信装置Ａ、Ｂそれぞれにおいて、図２に示されるような第２認証コードが既に登録されているか否かを判断する。認証コード記憶部７に第２認証コードが登録されていない場合、ステップＳ４、Ｓ１８に進み、認証データの演算に使用する認証コードを第１認証コードとしておく。

【００３５】

第２認証コードが既に登録されている場合、ステップＳ５、Ｓ１９において、無線通信装置Ａ、Ｂそれぞれにおいて、入力された第１認証データと認証コード記憶部７に記憶されている第１認証コードとが一致するか否かを判断する。両者

が不一致の場合は、認証に失敗したものとして処理を終了する。

【００３６】

ステップＳ５、Ｓ１９において、入力された第１認証コードと認証コード記憶部７に記憶されている第１認証コードとが一致した場合は、ステップＳ６、Ｓ２０に進み、認証データの演算に使用する認証コードを第２認証コードとしておく。

【００３７】

次に、発信元の無線通信装置Ａではステップ７において、乱数発生部５から認証用乱数を発生し、通信先の無線通信装置Ｂへ送信する。無線通信装置Ｂではステップ２１において、その認証用乱数を受信する。

【００３８】

次にステップＳ８、Ｓ２２において、無線通信装置Ａ、Ｂそれぞれにおいて認証用乱数、認証コード、無線通信装置Ｂの識別番号をパラメータとして、認証データを演算する。この認証コードは、初回の認証時（第２認証コードが未登録）はステップＳ４、Ｓ１８で設定された第１認証コードであり、２回目以降の認証時（第２認証コードが既登録）はステップＳ６、Ｓ２０で設定された第２認証コードである。

【００３９】

演算の結果生成された認証データを、ステップＳ２３において無線通信装置Ｂから発信元の無線通信装置Ａへ送信し、ステップＳ９において無線通信装置Ａが無線通信装置Ｂからの認証データを受信する。

【００４０】

無線通信装置Ａでは、ステップＳ９で受信した認証データとステップＳ８で演算の結果生成した認証データをステップＳ１０において照合する。一致していない場合、ステップＳ１１において認証不成功通知を通信相手の無線通信装置Ｂへ送信し、終了する。一致している場合、ステップＳ１２において認証成功通知を通信相手の無線通信装置Ｂへ送信し、ステップＳ１３に進む。

【００４１】

無線通信装置Ｂでは、ステップＳ２４において、無線通信装置Ａから送信され

た認証結果を受信する。ステップＳ２５において、認証が成功したか否か判定する。不成功の場合は、終了する。成功した場合は、ステップＳ２６に進む。

【００４２】

ステップＳ１３、Ｓ２６において、ステップＳ７、Ｓ２１で受け渡しをした認証用乱数と、認証コード記憶部７に記憶されている第２認証コードとから、無線通信装置Ａ、Ｂで同じ演算処理を行い、新たな第２認証コードを生成する。生成された第２認証コードは認証コード記憶部７に記憶され、第２認証コードが更新される。第２認証コードの演算方法としては、例えば認証用乱数と第２認証コードとの排他的論理和をとること等が考えられる。

【００４３】

その後、ステップＳ１４、Ｓ２７において、無線通信装置Ａ、Ｂ間で互いに通信データを送受信する。

【００４４】

再び認証を行なうときはステップＳ２からステップＳ１３、及びステップＳ１６からステップＳ２６を繰り返す。

【００４５】

ここで、認証データ演算のためのパラメータである認証用乱数と認証データとを無線で送受信している際に、第三者に傍受された場合を考える。従来と同様に、認証用乱数、認証データ、および無線通信装置Ｂの識別番号から、認証データの演算パラメータの一つである演算用認証コードが逆算されてしまう恐れがある。しかし、演算用認証コードは各認証後に更新（初回は第１認証コードが使われ、２回目以降の認証時は第２認証コード）されるので、認証の都度、通信を傍受して演算用認証コードを解析する必要があり、解析することは困難である。しかも、万が一、演算用認証コードが解析されたとしても、演算用認証コードとステップＳ１６で入力させる認証コードは別としているので、次回の認証をする際に、ステップＳ１６で解析結果を入力しても、ステップＳ１９の第１認証コードの照合で不一致となり、認証に失敗してしまう。これにより、第三者が通信を傍受して不正に認証コードを取得し、成り済まして通信をすることを防ぐことができる。

【００４６】

以上説明したように、第１実施形態によれば、認証の際に入力する認証コードと、実際に認証に使う認証コードとを別のものとし、さらに実際に認証に使う認証コードを認証の度、変更することにより、第三者が通信を傍受して認証に使った認証コードを解析したとしても、次回の認証の際には認証コードが更新されているので、解析した認証コードが無効となって、不正な通信を防ぐことができる。

【００４７】

変形例

なお、本願発明は上記実施形態に限定されるものではなく、実施段階ではその趣旨を逸脱しない範囲で種々に変形することが可能である。また、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題が解決でき、発明の効果の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【００４８】

上述の説明では、第２認証コードと無線通信装置Ａから無線通信装置Ｂへ送信された認証用乱数をパラメータとして所定の演算を行ない新しい第２認証コードを更新したが、第２認証コードの更新方法については、無線通信装置Ａと無線通信装置Ｂとで同じ演算方法により新しい認証コードを生成しさえすればよく、説明した方法に限定されない。

【００４９】

無線通信装置に限らず、有線の通信装置についても本発明は適用可能である。

【発明の効果】

以上説明したように、本発明によれば、所定のパラメータから演算され認証に使うデータを認証の度、変更することにより、第三者が通信を傍受して認証に使ったデータを解析したとしても、次回の認証の際には認証データが更新されているので、解析した認証データが無効となって、不正な通信を防ぐことができる。

【図面の簡単な説明】

【図１】

本発明による無線通信装置の第１実施形態の構成を示すブロック図。

【図２】

第１実施形態の認証コード記憶部に記憶されている認証コードを示す図。

【図３】

本発明による認証方法を示すフローチャート。

【符号の説明】

１…アンテナ

２…無線部

３…送信データ発生部

４…データ処理部

５…乱数発生部

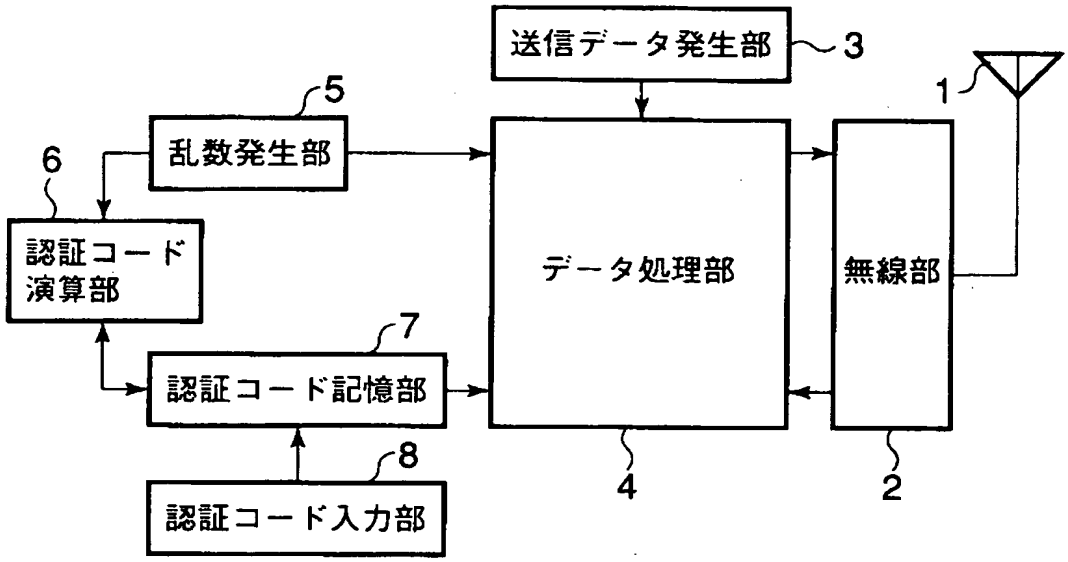
６…認証コード演算部

７…認証コード記憶部

８…認証コード入力部

【書類名】　　図面

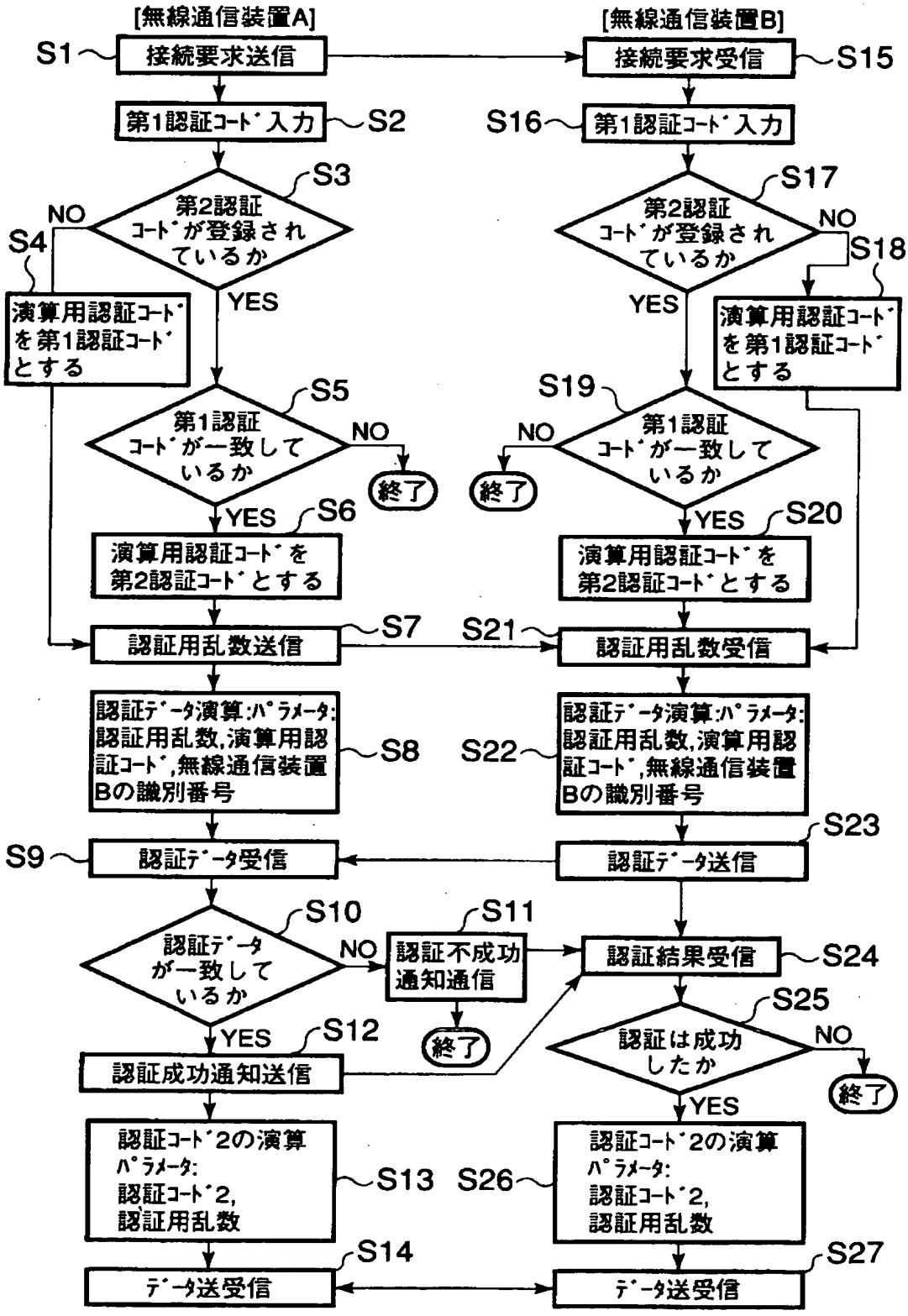
【図１】



【図２】

第1認証コード	無線通信装置識別番号	第2認証コード
01234567	0x004512736100	33258611
	0x003512880092	19378910
	0x003212747551	43279982
	0x001077793815	10127789
01234568	0x004512736100	48238710
	0x003512880092	11295022
	0x003212747552	33109814
	0x001077793814	27520013
・・・	・・・	・・・

【図３】


[無線通信装置A]
[無線通信装置B]
S1
接続要求送信
接続要求受信
S15
第1認証ｺｰﾄﾞ入力
S2
S16
第1認証ｺｰﾄﾞ入力
S3
第2認証ｺｰﾄﾞが登録されているか
NO
YES
S4
演算用認証ｺｰﾄﾞを第1認証ｺｰﾄﾞとする
S17
第2認証ｺｰﾄﾞが登録されているか
NO
YES
S18
演算用認証ｺｰﾄﾞを第1認証ｺｰﾄﾞとする
S5
第1認証ｺｰﾄﾞが一致しているか
NO
終了
YES
S6
演算用認証ｺｰﾄﾞを第2認証ｺｰﾄﾞとする
S19
第1認証ｺｰﾄﾞが一致しているか
NO
終了
YES
S20
演算用認証ｺｰﾄﾞを第2認証ｺｰﾄﾞとする
S7
認証用乱数送信
S21
認証用乱数受信
S8
認証ﾃﾞｰﾀ演算:ﾊﾟﾗﾒｰﾀ:認証用乱数,演算用認証ｺｰﾄﾞ,無線通信装置Bの識別番号
S22
認証ﾃﾞｰﾀ演算:ﾊﾟﾗﾒｰﾀ:認証用乱数,演算用認証ｺｰﾄﾞ,無線通信装置Bの識別番号
S23
S9
認証ﾃﾞｰﾀ受信
認証ﾃﾞｰﾀ送信
S10
認証ﾃﾞｰﾀが一致しているか
NO
S11
認証不成功通知通信
終了
認証結果受信
S24
S25
認証は成功したか
NO
終了
YES
S12
認証成功通知送信
S13
認証ｺｰﾄﾞ2の演算ﾊﾟﾗﾒｰﾀ:認証ｺｰﾄﾞ2,認証用乱数
S26
認証ｺｰﾄﾞ2の演算ﾊﾟﾗﾒｰﾀ:認証ｺｰﾄﾞ2,認証用乱数
S14
ﾃﾞｰﾀ送受信
S27
ﾃﾞｰﾀ送受信

【書類名】　　要約書

【要約】

【課題】傍受により認証データを演算するパラメータを取得し、成り済ましにより不正な通信を行なうことを防止する。

【解決手段】認証コード記憶部（７）と、認証コード記憶部（７）に記憶されている認証コードを用いて認証を行ない、認証が成功した場合、新たな認証コードを演算し、認証コード記憶部に記憶されている認証コードを更新するデータ処理部（４）とを具備する無線通信装置。入力された認証コードを第１の認証コードと照合し、両者が不一致の場合、認証を終了し、両者が一致した場合、データ処理部（４）を動作させる。

【選択図】　　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝